Linear Algebra and its Applications 432 (2010) 2381–2398

Contents lists available at ScienceDirect

Linear Algebra and its Applications

journal homepage: www.elsevier.com/locate/laa

Search for properties of the missing Moore graph

Martin Mačaj [a,*], Jozef Širáň [b,c]

[a] Comenius University, Bratislava, Slovakia
[b] Open University, Milton Keynes, UK
[c] Slovak University of Technology, Bratislava, Slovakia

ARTICLE INFO

Article history:
Received 30 April 2009
Accepted 13 July 2009
Available online 19 August 2009

Submitted by R.A. Brualdi

AMS classification:
05C50
05C25
20B25
20C15

Keywords:
Moore graphs
Spectral graph theory
Rational representations

ABSTRACT

In the degree-diameter problem, the only extremal graph the existence of which is still in doubt is the Moore graph of order 3250, degree 57 and diameter 2. It has been known that such a graph cannot be vertex-transitive. Also, certain restrictions on the structure of the automorphism group of such a graph have been known in the case when the order of the group is even. In this paper we further investigate symmetries and structural properties of the missing Moore $(57, 2)$-graph(s) with the help of a combination of spectral, group-theoretic, combinatorial, and computational methods. One of the consequences is that the order of the automorphism group of such a graph is at most 375.

1. Introduction

In graph theory there are a number of problems linking graphs with linear algebra and group theory. A prominent example that has been around for five decades is the *degree-diameter problem*. We recall that the *degree* of a vertex of a graph is the number of edges incident with the vertex, while the *diameter* of a graph is the smallest k such that any two vertices in the graph are connected by a path of length at most k. In its broadest formulation the degree-diameter problem is to find, for any given positive integers d and k, the largest order of a graph of maximum degree d and diameter k and classify the corresponding extremal graphs. Research in this area was initiated by the pioneering paper by Hoffman and Singleton [9], prompted by Moore who suggested the problem. By now the bibliography of related

* Corresponding author.
E-mail addresses: martin.macaj@fmph.uniba.sk (M. Mačaj), siran@math.sk (J. Širáň).

0024-3795/$ - see front matter © 2009 Elsevier Inc. All rights reserved.
doi:10.1016/j.laa.2009.07.018

papers, including those addressing analogues of the problem for structures such as digraphs and finite geometries, counts hundreds of papers. For history and details we refer to the relatively recent survey paper by Miller and the second author [11]. In what follows we only summarize the facts essential for our contribution.

A simple spanning tree argument [9] shows that the order of a graph of maximum degree d and diameter k cannot exceed $1 + d + d(d-1) + \cdots + d(d-1)^{k-1}$. This quantity is the *Moore bound* and graphs of order equal to the Moore bound are known as the *Moore* (d, k)*-graphs*. If $k = 1$ the Moore (d, k)-graphs are the complete graphs of order $d + 1$ for any $d \geqslant 1$. The other trivial cases are $d = 1$ and $d = 2$ where the Moore graphs are the complete graph of order two and cycles of length $2k + 1$ for any $k \geqslant 1$. Existence of Moore (d, k)-graphs for $d \geqslant 2$ and $k \geqslant 2$ turned out to be a hard problem that stimulates research until now. In [9] the authors proved that for $k = 2$, Moore (d, k)-graphs exist only if $k = 2$ and $d = 2, 3, 7$, and possibly 57, and that there are no Moore (d, k)-graphs for $k = 3$. In the first three cases the Moore graphs are unique, namely, the 5-cycle, the Petersen graph, and the Hoffman-Singleton graph. Non-existence of Moore (d, k)-graphs for $k \geqslant 4$ was proved independently by Bannai and Ito [2] and Damerell [5]. All these papers were based on an extensive use of methods of linear algebra and spectral methods in particular.

It is striking that all the known Moore (d, k)-graphs turn out to be vertex-transitive; in fact, their automorphism groups have rank 3. This has naturally led to investigation of symmetry properties of the hypothetical $(57, 2)$-Moore graph(s). For brevity, let Γ be a Moore $(57, 2)$-graph and let G be its automorphism group. The study of G was initiated by Aschbacher [1] by proving that G cannot be a rank 3 group. Later in a series of lectures for his graduate students, Graham Higman showed that Γ cannot be vertex-transitive; see Cameron's monograph [3] for an account of the proof. The same argument shows that the order of G is not divisible by 4. This was taken further by Makhnev and Paduchikh [10] by a closer investigation of the structure of G, assuming that G contains an involution. A consequence of their investigation is the bound $|G| \leqslant 550$ if G has even order.

The aim of this contribution is to further investigate possible symmetries (in conjunction with other properties) of the Moore $(57, 2)$-graph(s) the existence of which is still in doubt. Using a blend of spectral, group-theoretic, combinatorial, and computational methods we show that $|G|$ can assume only a very restricted set of values. In particular, we obtain the inequality $|G| \leqslant 375$ with no restriction on the parity of $|G|$.

The structure of the paper is as follows. The known properties of a Moore $(57, 2)$-graph Γ, with emphasis on symmetries, are reviewed in Section 2. In Sections 3 and 4 we present a selection of matrix methods used in investigation of automorphism groups of graphs and prove a number of general results tailored to our needs. In the interest of clarity, Section 5 contains arithmetic restrictions on characters and other related invariants of automorphisms of Γ. In Sections 6, 7 and 8 we derive upper bounds on orders of Sylow p-subgroups of the automorphism group G of Γ for odd primes. Finally, using solvability of G, in Section 9 we combine our results to determine possible orders of G. We conclude the paper by a handful of remarks.

In our study we use a wide range of methods. Attempting to keep the length of the paper within reasonable bounds we decided to omit definitions of some concepts that are considered generally known. We refer the reader to the monographs of Curtis and Reiner [4] for character theory, Godsil [8] for equitable partitions, Rotman [13] for general group theory, and Dixon and Mortimer [6] for permutation groups.

Groups of small order appearing in our investigation are described in form of direct and semi-direct products, except for groups of order 81 and 625 the description of which comes from the `SmallGroup` library of GAP [7].

2. The missing Moore graph: State-of-the-art

Throughout the paper we let Γ denote a Moore $(57, 2)$-graph with adjacency matrix A. General graph-theoretic terms will, in most cases, be used with reference to Γ, and to A whenever appropriate. We begin with listing a selection of basic properties of Γ that can be extracted from [9].

Proposition 1. *The graph Γ has* 3250 *vertices and girth* 5. *Its adjacency matrix A satisfies the equation $A^2 + A - 56I = J$, where J is the all-one matrix. Consequently, its eigenvalues are* 57, 7, *and* -8, *with multiplicities* 1, 1729, *and* 1520, *respectively*.

Any Moore graph of diameter 2 has girth 5 and therefore such graphs have the property that *any two vertices have 0 or exactly 1 common neighbor according as they are adjacent or not*. That is, Moore graphs of diameter 2 are exactly the strongly regular $(0, 1)$-graphs. If the regularity condition is omitted, then, apart from the trivial cases of an empty graph, an isolated vertex, or an isolated edge, the only other graphs with the above property are the stars $K_{1,n}$ for $n \geqslant 2$.

The starting point in the study of automorphisms of Moore graphs was an observation of Aschbacher [1] regarding fixed-point subgraphs. For a group X of automorphisms of Γ let $\mathrm{Fix}(X)$ be the subgraph induced by the set of all fixed points of X.

Lemma 1. *Let X be a group of automorphisms of Γ. Then,* $\mathrm{Fix}(X)$ *is empty, an isolated vertex, a pentagon, the Petersen graph, the Hoffman-Singleton graph, or a star $K_{1,n}$ for some $n \geqslant 1$.*

Since Γ has diameter 2, the image v^x of any vertex v under any automorphism x of Γ is either v itself, or a neighbor of v, or else a vertex at distance two from v. The following three numerical invariants related to this observation have turned out to be extremely useful. For $= 0, 1, 2$ let $a_i(x) = |\{v \in \Gamma;\ d(v, v^x) = i\}|$ where d stands for the distance. The main reason of success of spectral methods in the study of Moore graphs is, in fact, a close relation between the functions a_i and spectral properties of automorphisms of Γ, which we make explicit in Theorem 1.

Every permutation x of the vertex set of our Moore $(57, 2)$-graph Γ can be represented in the form of a permutation matrix P_x. As it is well known, x is an automorphism of Γ if and only if

$$P_x A = A P_x, \tag{1}$$

where A is the adjacency matrix of Γ. This induces a natural linear representation of $G = Aut(\Gamma)$ in the vector space generated by vertices of Γ, of dimension 3250, as well as on the eigenspaces corresponding to the three eigenvalues of Γ. By the fundamental observation of Higman, characters of these representations are closely related to combinatorial properties of automorphisms of Γ.

Theorem 1 (Higman; see [3]). *Let Γ be a Moore $(57, 2)$-graph with the adjacency matrix A. Let V_0, V_1, V_2 be the eigenspaces of A for eigenvalues* 57, 7, *and* -8, *respectively. Let X be an automorphism group of Γ and let χ_0, χ_1 and χ_2 be characters of the restriction of X onto V_0, V_1 and V_2, respectively. As before, for $x \in X$ let $a_i(x) = |\{v \in \Gamma;\ d(v, v^x) = i\}|$, $i = 0, 1, 2$. Finally, let $P = \begin{pmatrix} 1 & 1 & 1 \\ 57 & 7 & -8 \\ 3192 & -8 & 7 \end{pmatrix}$ and $Q = \frac{1}{3250}\begin{pmatrix} 1 & 1 & 1 \\ 1729 & 637/3 & -13/3 \\ 1520 & -640/3 & 10/3 \end{pmatrix}$. Then, $Q = P^{-1}$ and $(\chi_0(x), \chi_1(x), \chi_2(x))^T = Q(a_0(x), a_1(x), a_2(x))^T$.*

We recall that Higman demonstrated power of this theorem by showing that it implies that Γ cannot be vertex-transitive; see [3]. We will make use of the following two consequences.

Lemma 2 [3]. *Let x be an involutory automorphism of Γ. Then, $a_0(x) = 56$ and $a_1(x) = 112$. Consequently, the order of $Aut(\Gamma)$ is not divisible by* 4.

Lemma 3. *For any $x \in X$ we have*

$$\chi_1(x) = \frac{1}{15}(8a_0(x) + a_1(x) - 65)$$

and therefore

$$a_1(x) \equiv 7a_0(x) + 5 \bmod 15.$$

Proof. The first statement follows from the fact that $a_0(x) + a_1(x) + a_2(x) = 3250$. The congruence is a consequence of the fact that the algebraic integer $\chi_1(x)$ is, according to the first statement, also a rational number and therefore an integer. □

Makhnev and Paduchikh [10] investigated possible groups of automorphisms of Γ of even order and obtained the following result.

Theorem 2 [10, Theorem 1]. *Let Γ be a Moore $(57, 2)$-graph and let $G = \mathrm{Aut}(\Gamma)$. Assume that G contains an involution t. Then the following statements hold*:

(a) *$G = Y\langle t\rangle \times X$ for some subgroups X and Y of odd order, Y is inverted by t, and either $|Y|$ divides 5 or 57, or $|Y|$ divides 21,*
(b) *if $X \neq 1$, then $\mathrm{Fix}(X)$ can be one of the following: a star ($Y = 1$ and $|X| = 7$); a pentagon, in which case $|Y|$ divides 5 and $|X|$ divides 55; the Petersen graph, in which case $|Y|$ divides 3 and $|X|$ divides 27; and finally the Hoffman-Singleton graph, in which case Y divides 5 or 7 and X divides 25.*

The proof of this result is divided into a series of lemmas dealing with properties of involutory automorphisms of Γ. The series is preceded with the following more specific version of Lemma 1, a further extension of which is one of the cornerstones of our investigation.

Lemma 4. *Let X be a group of automorphisms of Γ of odd prime order. Then, one of the following holds*:

(1) $\mathrm{Fix}(X)$ *is empty and $|X|$ divides $13 \cdot 5$;*
(2) $\mathrm{Fix}(X)$ *is a singleton and $|X|$ divides $3 \cdot 19$;*
(3) $\mathrm{Fix}(X)$ *is a star with $|\mathrm{Fix}(X)| = 2 + 7l$ and $|X|$ divides 7;*
(4) $\mathrm{Fix}(X)$ *is a pentagon and $|X|$ divides $11 \cdot 5$;*
(5) $\mathrm{Fix}(X)$ *is the Petersen graph and $|X|$ divides 3;*
(6) $\mathrm{Fix}(X)$ *is the Hoffman-Singleton graph and $|X|$ divides 5.*

3. Equitable partitions

Equitable partitions are a useful tool in spectral analysis of graphs, see [8]. To the best of our knowledge, this tool has not been used in connection with Moore $(57, 2)$-graph(s). Since we are only interested in such graphs we will introduce the concepts related to equitable partitions just for this special case.

Let Γ be a Moore $(57, 2)$-graph and let $\mathcal{S} = \{S_1, S_2, \ldots, S_k\}$ be a partition of the vertex set of Γ. We say that $\mathcal{S}$ is an *equitable partition* of Γ if there exist integers b_{ij} such that each vertex from S_i has exactly b_{ij} neighbors in S_j. We say that the matrix $B = (b_{ij})_{k\times k}$ is the *adjacency matrix* of $\mathcal{S}$.

The most important but not the only instances of equitable partitions come from orbits of automorphism groups. For example, a different kind of equitable partition of Γ is obtained by taking, for any vertex v, the partition $\{\{v\}, N(v), \Gamma \setminus (N_v \cup \{v\})\}$ whose adjacency matrix is $\begin{pmatrix} 0 & 57 & 0 \\ 1 & 0 & 56 \\ 0 & 1 & 56 \end{pmatrix}$.

Spectral properties of the adjacency matrix of an equitable partition of a graph in general are closely related to the spectral properties of the adjacency matrix of the graph. In our special case, the property of being a Moore graph also manifests in the properties of the equitable partitions.

Lemma 5. *Let $\mathcal{S} = \{S_1, S_2, \ldots, S_k\}$ be an equitable partition of a Moore $(57, 2)$ graph Γ such that $|S_i| = s_i$ and let $B = (b_{ij})$ be the adjacency matrix of $\mathcal{S}$. Then*

(1) $s_i b_{i,j} = s_j b_{j,i}$;
(2) *57 is an eigenvalue of B with an eigenvector $(1, 1, \ldots, 1)^T$;*
(3) *the characteristic polynomial of B divides $(x - 57)(x - 7)^{1729}(x + 8)^{1520}$;*

(4) *coefficients* b_{ij}^k *of* B^k *are numbers of* k*-walks from a vertex of* S_i *into* S_j;
(5) $B^2 + B - 56I = (1, 1, \ldots, 1)^T(s_1, s_2, \ldots, s_k)$.

Proof. Items 1–4 follow directly from the general theory, cf. [8], and item 5 can be derived from 4 in a similar way as the equation $A^2 + A - 56I = J$ for the adjacency matrix A of Γ. □

Let X be an automorphism group of a Moore $(57, 2)$-graph Γ and let $B = (b_{i,j})$ be the adjacency matrix of the equitable partition formed by the orbits of X. For brevity we will say that B is the *adjacency matrix* of X. Moreover, for any matrix invariant of B we will say that the invariant is a property of X. That is, we will be speaking about the *trace* of X, *eigenvalues* of X, an so forth. Finally if O_i is the ith orbit of X we will say that the number $b_{i,i}$ is the *trace* of O_i. In general, we define the *trace* of a set of vertices S to be the average degree of the subgraph induced by S.

Let x be an element of X and let O be an orbit of X. We say that x *contributes* to O if for some vertex $v \in O$ the vertex v^x is adjacent to v; in symbols, $v^x \sim v$.

Lemma 6. *Let* O *be an orbit of* X *and let* $x \in X$ *contribute to* O. *Then*

(1) x^{-1} *contributes to* O;
(2) *if* $|X|$ *is odd, then* $\mathrm{Tr}(X)$ *is even*;
(3) *if* x *is central in* X, *then* $\mathrm{Tr}(O) \leqslant 2$;
(4) $\mathrm{Tr}(O)^2 < |O|$.

Proof. The first item is trivial and the second follows from the first. The third assertion follows from the fact that Γ has girth 5. Finally, for the last statement, let O be the ith orbit of X. By Lemma 5 we have $|O| = \mathrm{Tr}(O)^2 + \mathrm{Tr}(O) + \sum_{j \neq i} b_{i,j}b_{j,i} - 56 \geqslant \mathrm{Tr}(O)^2 + \mathrm{Tr}(O) + \sum_{j \neq i} b_{i,j} - 56 = \mathrm{Tr}(O)^2 + 1$. □

We omit the proof of the next straightforward observation.

Lemma 7. *If* $x \in X$ *is central and contributing to* O, *then* $|\{v \in O;\ v^x \sim v\}| = |O|$.

As we have indicated, Moore graphs exhibit surprising relations between their seemingly independent invariants. The following two lemmas are another illustration of this feature.

Lemma 8. *Let* X *have* k *orbits on* Γ. *Then*

$$\mathrm{Tr}(X) \equiv -8(k - 10) \bmod 15.$$

Proof. By Lemma 5 the eigenvalues of X are 57, 7, and -8, with 57 of multiplicity exactly one. If the multiplicity of 7 is one and -8 appears with multiplicity $k - 2$, then the trace of X is $64 - 8(k - 2) = -8(k - 10)$. Any replacement of -8 by 7 changes the trace by 15. □

Lemma 9. (1) *Let* O *be an orbit of* X *and let* $v \in O$. *Then* $\mathrm{Tr}(O) = |\{x \in X;\ v \sim v^x\}||O|/|X|$.
(2) $|X|\mathrm{Tr}(X) = |\{(x, v) \in X \times \Gamma;\ v \sim v^x\}| = \sum_{x \in X} a_1(x)$.

Proof. Let v be an element of O. By definition, $\mathrm{Tr}(O)$ is the number of neighbors of v in O. Any such neighbor is of the from v^x for $X_v = |X|/|O|$ elements of X. This proves the first statement; the second one is a direct consequence of the first. □

A further illustration of the power of spectral methods are the following estimates.

Lemma 10. *For any* $S \subseteq V(\Gamma)$ *we have*

$$-8 + \frac{|S|}{50} \leqslant \mathrm{Tr}(S) \leqslant 7 + \frac{|S|}{65}.$$

Proof. By [12, Lemma 4.1] we have

$$(57-7)\frac{|S|(3250-|S|)}{3250} \leqslant e(S,\Gamma\setminus S) \leqslant (57+8)\frac{|S|(3250-|S|)}{3250},$$

where $e(U,V)$ is the number of edges between the sets U and V. The result now follows from the fact that $e(S,\Gamma\setminus S) = |S|(57-\mathrm{Tr}(S))$. □

Corollary 1. *For any $x \in X$ we have $a_1(x) \leqslant 500$.*

Proof. Let $S = \{v \in \Gamma;\ v \sim v^x\}$. Clearly $a_1(x) = |S|$. If for some $u, v \in S$ we have $v^x \neq u \sim v \neq u^x$, then we have in Γ a quadrangle $u \sim v \sim v^x \sim u^x \sim u$. Therefore $\mathrm{Tr}(S) \leqslant 2$ and $a_1(x) = |S| \leqslant 50(8+2) = 500$. □

4. Characters

Because of the fact that Γ has integral eigenvalues, all its eigenspaces have bases over the field of rational numbers. Linear representations of Γ over these eigenspaces are therefore rational representations. Although the field of rational numbers is not algebraically closed, thanks to the fact that its characteristic is zero one still may use Maschke's Theorem (see [4]) on decompositions into irreducible rational representations. We would like to emphasize that by *irreducible rational representations* we mean rational representations irreducible over the field of rational numbers.

Besides Maschke's Theorem we will be using the following properties. Let us recall that two elements x, y of a group H will be said to belong to the same *rational class* of H if and only if the cyclic groups $\langle x\rangle$ and $\langle y\rangle$ are conjugate subgroups of H.

Theorem 3 [4]. *Let H be a finite group. Then, any rational representation of H is constant on all rational classes of H and the number of irreducible rational representations of H is equal to the number of rational classes of H.*

Proposition 2. *Let H be a finite group and let $x_1, x_2, \ldots, x_u$ be representatives of rational classes of H. Let $R_1, R_2, \ldots, R_u$ be irreducible $\mathbb{Q}$-representations of X with characters $r_1, r_2, \ldots, r_u$. Then, for any rational representation R of H with character χ the system of linear equation with the matrix*

$$\left(\begin{array}{cccc|c} r_1(x_1) & r_2(x_1) & \ldots & r_u(x_1) & \chi(x_1) \\ r_1(x_2) & r_2(x_2) & \ldots & r_u(x_2) & \chi(x_2) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ r_1(x_u) & r_2(x_u) & \ldots & r_u(x_u) & \chi(x_u) \end{array}\right)$$

has a solution in non-negative integers.

Proof. It is sufficient to realize that if a decomposition of R into irreducible rational representations contains n_i copies R_i for $1 \leqslant i \leqslant u$, then $\chi = n_1 r_1 + n_2 r_2 + \cdots + n_u r_u$. □

Combining Theorems 3 and 1 we immediately obtain:

Lemma 11. *Let X be an automorphism group of a Moore $(57,2)$-graph Γ. Then, the functions a_0, a_1, and a_2 are constant on rational classes of X.*

Proof. It is sufficient to observe that the values $a_i(x)$ are linear combinations of $\chi_j(x)$, which are characters of rational representations of X. □

In the next section we will apply Proposition 2 to the representation of X with the character χ_1 from Theorem 1 to specify values of the function a_1.

We conclude with an interesting observation. By Proposition 2, decomposition of a rational representation into irreducibles is determined by its character. The decomposition of the representation of X on Γ is determined by the function a_0. This means that if one knows all permutation representations of X together with their decompositions, then the values of a_0 impose stronger restrictions on the structure of orbits of X on Γ than the ones impled by the orbit counting lemma. Although we did not use this observation in our paper, we believe that it can be helpful in further research.

5. Tables

In previous sections we derived algebraic tools for obtaining restrictions on values of a_0, a_1 and a_2. In this section we will apply the tools for cyclic groups. There are two reasons for this restriction. Firstly, results for cyclic groups are sufficient for our purposes. Secondly, non-commuting elements influence each other to a much smaller extent than commuting ones, as one can observe already on non-Abelian groups of order pq.

Lemma 12. *Let x be an automorphism of a Moore $(57, 2)$-graph Γ of prime order p. Then, the values $a_1(x)$ and $\chi_1(x)$ satisfy*:

$a_0(x)$	p	$a_1(x)$	$\chi_1(x)$
0	5	$50 + 75k \leqslant 500$	$-1 + 5k$
0	13	$65 + 195k \leqslant 500$	$13k$
1^*	3	$27 + 45k = 0$	
1	19	$57 + 285k \leqslant 500$	$19k$
5	5	$10 + 75k \leqslant 500$	$-1 + 5k$
5	11	$55 + 165k \leqslant 500$	$2 + 11k$
10	3	0	1
50	5	$25 + 75k \leqslant 350$	$24 + 5k$
56	2	112	33
2	7	$49 + 105k \leqslant 500$	$7k$
9	7	$98 + 105k \leqslant 500$	$7 + 7k$
16	7	$42 + 105k \leqslant 500$	$7 + 7k$
23	7	$91 + 105k \leqslant 500$	$14 + 7k$
30	7	$35 + 105k \leqslant 500$	$14 + 7k$
37	7	$84 + 105k \leqslant 392$	$21 + 7k$
44	7	$28 + 105k \leqslant 260$	$21 + 7k$
51	7	77	28
58^*	7	$21 + 105k \leqslant 0$	

In particular, the starred cases $p = 3, a_0(x) = 1$ and $p = 7, a_0 = 58$ cannot occur.

Proof. By Lemma 3 and Theorem 1, we have $a_1(x) = 7a_0(x) + 5 + 15l$ for some $l \in \mathbb{Z}$ and $\chi_1(x) = -4 + a_0(x) + l$. By Proposition 2 applied to the cyclic group $\langle x \rangle$, the parameter l must be such that the system $\left(\begin{smallmatrix} 1 & p-1 & | & 1729 \\ 1 & -1 & | & \chi_1(x) \end{smallmatrix}\right)$ has a solution in non-negative integers. Values in the table are presented in such a way that k is non-negative. The general bound $a_1(x) \leq 500$ follows from Corollary 1.

The value of $a_1(x)$ for $p = 2$ is taken from [3]. If $p = 3$ and $a_1(x) > 0$ then Γ would contain a triangle, a contradiction. If $p = 7$ and $a_0(x) = 2 + 7m$, then there are only $56 * (8 - m)$ orbits of size 7 not connected with $\mathrm{Fix}(x)$ and x can contribute to at most one third of them. The arguments are similar for the cases $p = 19, a_0(x) = 1$, and $p = 5, a_0(x) = 50$. □

Lemma 13. *Let x be an automorphism of Γ of order p^2 where $p = 3$ or $p = 5$. Then, the values $a_1(x)$, $a_1(x^p)$, and $\mathrm{Tr}(\langle x\rangle)$ satisfy*:

p	$a_0(x)$	$a_0(x^p)$	$a_1(x)$	$a_1(x^p)$	$\mathrm{Tr}(\langle x\rangle)$
5	0	0	$50+75k$	$125+375l$	$60+60k+60l \leqslant 260$
5	0	50	$50+75k$	100	$56+60k \leqslant 276$
5	5	50	$10+75k$	100	$24+60k \leqslant 244$
5	50	50	$25+75k$	100	$36+60k \leqslant 56$
3	1	10	$27+45k$	0	$18+30k$
3	10	10	$45k$	0	$30k$

Proof. By Lemma 3 and Theorem 1 we have $a_1(x) = 7a_0(x) + 5 + 15l'$ and $\chi_1(x) = -4 + a_0(x) + l'$ for some $l' \in \mathbb{Z}$. By Proposition 2 applied to the cyclic group $\langle x\rangle$, the system $\left(\begin{array}{ccc|c} 1 & p-1 & p^2-p & 1729 \\ 1 & p-1 & -p & \chi_1(x^p) \\ 1 & -1 & 0 & \chi_1(x) \end{array}\right)$ has a solution in non-negative integers. Solving the system we obtain the table:

p	$a_0(x)$	$a_0(x^p)$	$a_1(x)$	$a_1(x^p)$	$\chi_1(x)$	$\chi_1(x^p)$	$\mathrm{Tr}(\langle x\rangle)$
5	0	0	$50+75k$	$125+375l$	$-1+5k$	$4+25l$	$60+60k+60l$
5*	0	5	$50+75k$	$85+375l$	$-1+5k$	$4+25l$	$33,6+60k+60l$
5	0	50	$50+75k$	$100+375l$	$-1+5k$	$29+25l$	$56+60k+60l$
5*	5	5	$10+75k$	$85+375l$	$-1+5k$	$4+25l$	$21,6+60k+60l$
5	5	50	$10+75k$	$100+375l$	$-1+5k$	$29+25l$	$24+60k+60l$
5	50	50	$25+75k$	$100+375l$	$24+5k$	$29+25l$	$36+60k+60l$
3	1	10	$27+45k$	0	$-2+3k$	1	$18+30k$
3	10	10	$45k$	0	$1+3k$	1	$30k$

The lines marked by a star require non-integral traces and therefore cannot occur.

If $|\mathrm{Fix}(\langle x^5\rangle)| = 50$, then 2500 vertices are adjacent to $\mathrm{Fix}(\langle x^p\rangle)$ and therefore $a_1(x^5) \leqslant 700/2$.

Finally, every orbit of size 25 adjacent to $\mathrm{Fix}(\langle x\rangle)$ has trace equal 0, which implies the upper bound on $\mathrm{Tr}(\langle x\rangle)$. □

Remark. Later in Proposition 3 we will show that the case $a_0(x) = 50$ cannot occur.

Lemma 14. *Let $X = P \times Q$ be an automorphism group of Γ such that P (Q) acts semi-regularly on $\Gamma \setminus \mathrm{Fix}(P)$ ($\Gamma \setminus \mathrm{Fix}(Q)$) and $(|P|, |Q|) = 1$. Then, for any central element $x \in X$,*

$$a_1(x) \equiv b_1(x) \bmod |X|, \tag{2}$$

where $b_1(x) = |\{v \in \mathrm{Fix}(P) \cup \mathrm{Fix}(Q);\ v \sim v^x\}|$. Moreover, if $x = x_P x_Q$ for $x_P \in P, x_Q \in Q$, then $b_1(x) = b_1(x_P) + b_1(x_Q)$.

Proof. As X acts semi-regularly on $\Gamma \setminus (\mathrm{Fix}(P) \cup \mathrm{Fix}(Q))$, the congruence (2) follows from Lemma 6. Since the kernel of the action of X on $\mathrm{Fix}(P)$ ($\mathrm{Fix}(Q)$) is exactly P (Q), we have $b_1(x) = b_1(x_P) + b_1(x_Q)$. □

Lemma 15. *Let x be an automorphism of Γ of order pq, where $p \leqslant q$ are primes. Assume that the values pq, $a_0(x)$, $a_0(x^p)$, and $a_0(x^q)$ are as in the first four columns of the table below. Then the values $a_1(x)$, $a_1(x^p)$, $a_1(x^q)$, and $\mathrm{Tr}(\langle x\rangle)$ satisfy*:

pq	$a_0(x)$	$a_0(x^p)$	$a_0(x^q)$	$a_1(x)$	$a_1(x^p)$	$a_1(x^q)\mathrm{Tr}(\langle x\rangle)$	
6	2	10	56	$4+90k$	0	112	$20+30k$
10	1	5	56	$102+150k$	$10+150l$	112	$56+60k+60l$
10	6	50	56	$62+150k$	$100+150l$	112	$76+60k+60l$
14	7	9	56	$84+210k$	$98+210l$	112	$86+90k+90l\leqslant 400$
14	14	16	56	$28+210k$	$42+210l$	112	$38+90k+90l\leqslant 344$
14	21	23	56	$182+210k$	$196+210l$	112	$170+90k+90l\leqslant 288$
14	28	30	56	$126+210k$	$140+210l$	112	$122+90k+90l\leqslant 232$
14	35	37	56	$70+210k$	$84+210l$	112	$74+90k+90l\leqslant 176$
14	42	44	56	$14+210k$	$28+210l$	112	$26+90k+90l\leqslant 120$
14*	49	51			182		
22	1	5	56	222	220	112	206
15	0	0	10	$5+75k+225m$	$50+75k$	0	$16+60k+120m$
35	1	16	50	$42+105k$	$147+105k$	175	$74+90k\leqslant 186$
35*	1	51	50	252	77	175	$206\leqslant 186$
55	5	5	5	55	55	385	78
65*	0	0	0			650	

Moreover, the cases marked by a star cannot occur.

Proof. We need to solve the system $\left(\begin{array}{cccc|c} 1 & p-1 & q-1 & (p-1)(q-1) & 1729 \\ 1 & -1 & q-1 & 1-q & \chi_1(x^q) \\ 1 & p-1 & -1 & 1-p & \chi_1(x^p) \\ 1 & -1 & -1 & 1 & \chi_1(x) \end{array}\right)$ in non-negative integers. Existence of an integral solution is equivalent to the conditions

$$p|\chi_1(x^p)-\chi_1(x), \tag{3}$$
$$q|\chi_1(x^q)-\chi_1(x), \tag{4}$$
$$pq|1729-\chi_1(x^p)-\chi_1(x^q)+\chi_1(x). \tag{5}$$

After solving the system with the help of Lemmas 12 and 14 and applying the arguments used in the proof of Lemmas 12 and 13 we obtain the table. Upper bounds on traces follows from facts that every orbit in Abelian group has trace at most 2 and that every orbit connected to $\mathrm{Fix}(\langle x\rangle)$ has trace equal to 0.

As an illustration we show details for the case $pq=35$, $a_1(x)=1$, $a_1(x^5)=16$ and $a_1(x^7)=50$. From the properties of the automorphism group of the Hoffman-Singleton graph we obtain $b_1(x^5)=7$, $b_1(x^7)=0$ and $b_1(x)=7$. Further, Lemmas 12 and 14 yield $a_1(x^5)=42+105l$, $\chi_1(x^5)=7+7l$, $a_1(x^7)=175$, and $\chi_1(x^7)=34$. Similarly $a_1(x)=42+105k$ and $\chi_1(x)=-1+7k$. Moreover, the condition (3) implies $l=1+k+5m$, that is, $a_1(x^5)=147+105k+525m$ (observe that the only solution with $m\neq 0$ is $k=4$ and $m=-1$).

The group $X=\langle x\rangle$ has on the subgraph $\mathrm{Fix}(\langle x^5\rangle)\cup\mathrm{Fix}(\langle x^7\rangle)$ one orbit of size 1, 3 orbits of size 5 and 6 orbits of size 7. Out of these orbits exactly three, of size 7 each, have trace equal to 2 while the others have trace equal to 0. The remaining points of Γ form 91 orbits of size 35, one of which is adjacent to $\mathrm{Fix}(X)$. Therefore $\mathrm{Tr}(X)\leqslant 6+90*2=186$, which implies $m=0$ and $k\leqslant 1$. □

6. p-Groups of automorphisms

In their proof of Lemma 4, Makhnev and Paduchikh exploited the observation that non-trivial orbits of an automorphism of a prime order p have length p and their argument is based on counting orbits around a suitably chosen fixed vertex. Realizing that the size of a non-trivial orbit of some p-group is a power of p, one can not only extend Lemma 4 to p-groups but also derive an upper bound on the size of a p-group with a given set of fixed points. Our findings are divided into four statements. Since the proof techniques are repetitious we only include a proof for Lemma 18.

Lemma 16. *Let X be a group of automorphisms of Γ such that X is a p-group for some odd prime p. Then, one of the following holds*:

(1) $\mathrm{Fix}(X)$ *is empty and* $p \in \{5, 13\}$;
(2) $\mathrm{Fix}(X)$ *is a singleton and* $p \in \{3, 19\}$;
(3) $\mathrm{Fix}(X)$ *is a star with* $|\mathrm{Fix}(X)| = 2 + 7l$ *and* $p = 7$;
(4) $\mathrm{Fix}(X)$ *is a pentagon and* $p \in \{5, 11\}$;
(5) $\mathrm{Fix}(X)$ *is the Petersen graph and* $p = 3$;
(6) $\mathrm{Fix}(X)$ *is the Hoffman-Singleton graph and* $p = 5$.

Lemma 17. *Let X be a an automorphism group of Γ of order 3^k. Then one of the following holds*:

(1) $\mathrm{Fix}(X)$ *is the Petersen graph and* $|X|$ *divides* 27;
(2) $\mathrm{Fix}(X)$ *is a singleton and* $|X|$ *divides* 81.

For any vertex v of Γ we let $N(v)$ denote the set of the 57 neighbors of v.

Lemma 18. *Let X be a group of automorphisms Γ such that $|X|$ is a 5-group. Then one of the following holds*:

(1) $\mathrm{Fix}(X)$ *is the Hoffman-Singleton graph and* $|X|$ *divides* 25;
(2) $\mathrm{Fix}(X)$ *is a pentagon and* $|X|$ *divides* 125;
(3) $\mathrm{Fix}(X)$ *is empty and* $|X|$ *divides* 5^6.

Proof. (1) Let $a \in \mathrm{Fix}(X)$. If there was an orbit O in $N(a) \setminus \mathrm{Fix}(X)$ such that $|O| < |X|$, then for any element $o \in O$ the point stabilizer X_o of o would be a proper subgroup of X with $|\mathrm{Fix}(X_o)| > 50$, a contradiction. Therefore, X act semi-regularly on $N(a) \setminus \mathrm{Fix}(X)$ and $|X|$ divides $|N(a) \setminus \mathrm{Fix}(X)| = 50$.

(2) Let $a \in \mathrm{Fix}(X)$. Since $|N(a) \setminus \mathrm{Fix}(X)| = 55$, the group X has on $N(a) \setminus \mathrm{Fix}(X)$ an orbit O of size 5. Let Y be a point stabilizer in this orbit. If $Y \neq X$, then $\mathrm{Fix}(Y)$ is the Hoffman-Singleton graph and by (1) we have $|Y| \leqslant 25$ and $|X| = 5|Y| \leqslant 125$.

(3) As $3250 \equiv 125 \bmod 625$, the smallest orbit of X on Γ has size at most 125. Let Y be a point stabilizer in this orbit. If $Y \neq X$, then $\mathrm{Fix}(Y)$ is a pentagon or the Hoffman-Singleton graph and by (1) or (2) we have $|Y| \leqslant 125$ and $|X| = 125|Y| \leqslant 5^6$. □

Lemma 19. *Let $p > 5$ be a prime and let X be a group of automorphisms of Γ of order p^k. Then one of the following holds*:

(1) $\mathrm{Fix}(X) = \emptyset$ *and* $X \cong \mathbb{Z}_{13}$;
(2) $\mathrm{Fix}(X)$ *is a singleton and* $X \cong \mathbb{Z}_{19}$;
(3) $\mathrm{Fix}(X)$ *is a pentagon and* $X \cong \mathbb{Z}_{11}$;
(4) $\mathrm{Fix}(X)$ *is a star on* $2 + 7l$ *vertices and* $X \cong \mathbb{Z}_7$;
(5) $\mathrm{Fix}(X)$ *is an edge and* $X \cong \mathbb{Z}_7 \times \mathbb{Z}_7$.

With the help of further trickery, in the next section we will push down the bound on the order of a 3-group X acting on Γ from Lemma 17 in the case when $\mathrm{Fix}(X)$ is a singleton. Likewise, in Section 8 we will decrease the upper bound on orders of 5-groups acting on Γ for any possible fixed subgraphs.

Theorem 4. *Let X be a group of automorphisms of Γ of order 3^k. Then, $k \leqslant 3$.*

Theorem 5. *Let X be a group of automorphisms of Γ of order a power of* 5. *Then one of the following holds*:

(1) $\mathrm{Fix}(X)$ *is the Hoffman-Singleton graph and* $|X|$ *divides* 5;
(2) $\mathrm{Fix}(X)$ *is a pentagon and* $|X|$ *divides* 25;
(3) $\mathrm{Fix}(X)$ *is empty and* $|X|$ *divides* 125.

The proofs will require extension of our methods by considering a few general tools regarding group actions on sets.

Let O be an orbit of an action of a group X on a set and let X_o be a stabilizer of an element $o \in O$. Then, the stabilizers of all points in O are precisely the conjugates of X_o in X. In this notation we have an observation a proof of which is left to the reader:

Lemma 20. *In the above notation, let* $\mathrm{Conj}(X_o)$ *be the number of conjugates of* X_o *in* X. *Then,* $|\mathrm{Fix}(X_o) \cap O| \cdot \mathrm{Conj}(X_o) = |O|$.

Recall that the *core* $\mathrm{Core}(X_o)$ of X_o in X is the intersection of all the conjugates of X_o in X. Since $\mathrm{Core}(X_o)$ is independent of the choice of $o \in O$, we will denote this subgroup by $\mathrm{Core}(O)$ and call it the *core of* O.

7. Proof of Theorem 4

By Lemma 17 it is sufficient to deal with the case $\mathrm{Fix}(X) = \{a\}$. We begin with a slightly more general auxiliary result.

Lemma 21. *Let* Γ *admit a* 3*-group* X *of automorphisms with* $\mathrm{Fix}(X) = \{a\}$ *and let* x *be a non-trivial element of* X. *Then,*

(1) *if* X *has (at least) two orbits of size* 3 *on* $N(a)$, *then* $|X| = 9$, *and*
(2) *if* X *has an orbit of size* 9 *on* $N(a)$, *then* $|X| \leqslant 27$.

Proof. (1) Let O_1, O_2 be two orbit of size 3 on $N(a)$, let $o_1 \in O_1$, $o_2 \in O_2$, and let X_1 and X_2 be vertex stabilizers of o_1 and o_2 in X, respectively. Then, X_1 and X_2 are normal subgroups of index 3 in X and their intersection is a normal subgroup of index 9 in X. Moreover, every element of $X_1 \cap X_2$ fixes at least 6 elements in $N(a)$. Therefore $|X_1 \cap X_2| = 1$ and $|X| = 9$.

(2) Let $|X| > 9$, let O be an orbit of size 9 in $N(a)$, let $o \in O$ and let $o' \in O \setminus \mathrm{Fix}(o)$. Denote by $X_{oo'}$ the vertex stabilizer of o' in X_o. Then, similarly to the case (1)), $|X_{oo'}| = 1$ and $|X| = [X : X_{oo'}] = |O| \cdot |o'^{X_o}| = 9 \cdot 3 = 27$. □

Corollary 2. *If* $|X| = 81$, *then* X *is isomorphic to the group* `SmallGroup(81,9)` *of the GAP library*.

Proof. If $|X| = 81$, then X acts on $N(a)$ with two orbits of size 27 and one orbit of size 3. Conjugacy classes of vertex stabilizers in orbits of size 27 are distinct and, by Lemma 20, each has 9 elements. Examining the lattices of subgroups of groups of order 81 with the help of *GAP* one can check that $X = \mathtt{SmallGroup}(81, 9)$ is the only group with at least two such conjugacy classes. □

We are now in position to prove Theorem 4 stated in section 6 on the upper bound 27 for the order of a 3-group acting on Γ.

Proof of Theorem 4. The arguments are a combination of the previous observations with computational results facilitated by GAP. Letting $X = \mathtt{SmallGroup}(81, 9)$, one finds that X has five conjugacy classes of subgroups of order three, of sizes 1, 3, 9, 9 and 9. The two classes of size 9 are vertex stabilizers in orbits of size 27 while the remaining elements of order 3 together with the identity element form a subgroup of order 27. As every element of order 3 in X fixes the Petersen graph, this group of order 27 is the vertex stabilizer in orbits of size 3. Consequently, X has 48 orbits in total, one of size 1, three of size 3, six of size 27 and the remaining 38 orbits have size 81. By Lemma 8 we have $\mathrm{Tr}(X) = 26 + 30l$.

Cyclic subgroups of order 9 form a single conjugacy class of X of size 3. Therefore, the function a_1 is constant on elements of order 9, and, by Lemma 9, for any x of order 9 we have $81\mathrm{Tr}(X) = 18a_1(x)$, that is, $a_1(x) = 117 + 135l$.

Any coset of an orbit stabilizer which contains an element of order 9 also contains an element of order 3. Elements of order 9 therefore contribute only to orbits of size 81.

All elements of order 9 in X lie in the common subgroup Y of X, isomorphic to $\mathbb{Z}_9 \times \mathbb{Z}_3$. Every orbit of X of size 81 splits into three orbits of Y of size 27, therefore by Lemma 7, $a_1(x)$ is a multiple of 27 – a contradiction. □

8. Proof of Theorem 5

We begin with auxiliary results some of which are of independent interest.

Proposition 3. *Let X be a group of automorphisms of a Moore $(57,2)$-graph Γ of order a power of 5. If $\mathrm{Fix}(X)$ is the Hoffman-Singleton graph, then $|X| \leqslant 5$.*

Proof. Let us assume that $|X| = 25$. The semi-regular action of X on $\Gamma \setminus \mathrm{Fix}(X)$ gives 50 orbits of size 1 and 128 orbits of size 25. In the neighborhood of any fixed point of X there are exactly two orbits of size 25 and both have trace equal to 0. As X is Abelian and has odd order, each of the remaining 28 orbits of size 25 has trace equal to 0 or 2. The trace of X therefore does not exceed 56. Moreover, the trace is even and congruent to $-8 \cdot 168 \equiv 6 \bmod 15$. It follows that at least one of these 28 orbits has trace equal to 0.

Let us order the orbits of X in such a way that $O_1, \ldots, O_{50}$ are the fixed points of X, points in O_{50+i} and O_{100+i} lie in the neighborhood of O_i $(i = 1, 2, \ldots, 50)$, and let O_{178} be an orbit with zero trace. Let $B = (b_{i,j})$ be the adjacency matrix of X. By Lemma 5, B satisfies the equality

$$B^2 + B - 56I = (1, 1, \ldots, 1)^T (s_1, s_2, \ldots, s_k). \tag{6}$$

We will analyze the way the entry in the bottom right corner in the matrix on the right-hand side of this equality is obtained.

We begin with looking at the entries $b_{178,j}$. Since O_{178} is not connected to $\mathrm{Fix}(X)$, we have $b_{178,i} = 0$ for $1 \leqslant i \leqslant 50$. Let i be a vertex of $\mathrm{Fix}(X)$, $1 \leqslant i \leqslant 50$. Since Γ is a Moore graph, every vertex in O_{178} is adjacent to precisely one vertex in $O_{50+i} \cup O_{100+i}$. This means that $b_{178,50+i} + b_{178,100+i} = 1$ for every $i = 1, 2, \ldots, 50$. As every vertex in O_{178} has degree 57 and $b_{178,178} = 0$, we have

$$\sum_{i=151}^{177} b_{178,i} = 7. \tag{7}$$

By semi-regularity of the action of X on $\Gamma \setminus \mathrm{Fix}(X)$ it further follows that $b_{178,j} = b_{j,178}$. Substituting all this information into (6) yields

$$\sum_{i=151}^{177} b_{178,i}^2 = 31. \tag{8}$$

Eqs. (7) and (8), have, however, no simultaneous solution in non-negative integers. □

This proves part (1) of Theorem 5. Part (2) follows from (1) in much the same way as in Lemma 18. The third part will be proved by demonstrating non-existence of a group of order 625. Details of the proof depend on the size of the smallest orbit. Note that part (2) of Theorem 5 implies that the smallest orbit size cannot be equal to 5.

Lemma 22. *If X is a group of automorphisms of Γ of order 625 and with the smallest orbit size 25, then X is isomorphic to* `SmallGroup(625,12)` *of the GAP library.*

Proof. Let O be an orbit of X of size 25 and let X_o be the vertex stabilizer of a vertex $o \in O$. Then $|X_o| = 25$ and, by Proposition 3, $|\mathrm{Fix}(X_o)| = 5$. Therefore $\mathrm{Fix}(X_o) \subseteq O$, X_o has five conjugates in X and O is unique orbit with stabilizer X_o. In particular X is not Abelian.

Let $p \in O \setminus \mathrm{Fix}(X_o)$. Then $|X_{op}| = 5$, therefore $\mathrm{Fix}(X_{op})$ is a copy of the Hoffman-Singleton graph and $O \subset X_{op}$. The remaining points of $\mathrm{Fix}(X_{op})$ either form another orbit of size 25, or there exists an orbit of size 125 such that X_{op} is a stabilizer of a vertex in this orbit.

If $Core(O) = X_{op}$, then X_{op} is normal in X and cannot be the vertex stabilizer of an orbit of size 125. Therefore there exists a unique orbit $O' \neq O$ with $Core(O') = Core(O) = X_{op}$.

There are 10 non-Abelian groups of order 625, their indexes in the SmallGroup library being 3, 4, 6, 7, 8, 9, 10, 12, 13, 14. Groups 6 and 14 are excluded since they have only normal subgroups of

order 25. In groups 3, 4, 9, 10, 12, 14 all non-normal subgroups of order 25 have core of size 5. The number of cores must be a multiple of 5, which is true only for the groups 3 and 12, in both cases there are five cores. However in the group 3 one core lies in six classes of groups and remaining four cores lies in 1 class each, whereas we need every core to lie in two conjugacy classes of groups of order 25 (which holds in the group 12).

It remains to exclude groups 7 and 8. In these groups there are six conjugacy classes of subgroups of order 25 with core of size 5; moreover, here the core is always the centre of the group. There are also five classes with trivial core. Therefore there are exactly five orbits of size 25 and the number of orbits with a non-trivial core is either 0 or 2.

In both cases the centre has order 5 and the Frattini subgroup is elementary Abelian of order 25 and contains the centre. If f is a non-central element from the Frattini subgroup, then every conjugacy class of subgroups of order 25 with trivial core has a subgroup containing f, and f has five conjugates in X.

It follows that in every orbit O of size 25 with a trivial core there exists an element o fixed by f and $|\mathrm{Fix}(\langle f\rangle) \cap O| = 5$. If f generates the stabilizer of a vertex in an orbit of size 125, then it fixes 25 elements of this orbit. Hence the possibility that X has exactly three orbits of size 5 with a trivial core cannot occur. Thus, there are five orbits of size 25, and all stabilizers have trivial core (and are distinct).

Let O be an orbit of size 25 with a trivial core. The conjugacy classes of subgroups consisting of stabilizers of vertices from O comprise five groups any two of which intersect non-trivially while any three have trivial intersection. This implies that for any pair of points $o, p \in O$ such that $p \notin X_o$, the subgroup X_{op} fixes a Hoffman-Singleton graph and $\mathrm{Fix}(X_{op})$ contains exactly 10 elements of O. As X_{op} has five conjugates in X, it cannot be the vertex stabilizer of an orbit of size 125 (it would fix 25 points of this orbit and the equation $50 = 25a + 10b$ has no solutions in $\mathbb{N}$). Therefore X_{op} fixes 10 points from every orbit of size 25. Consequently, the system of subgroups X_{op}, which is the system of intersections of pairs of vertex stabilizers of elements in O, do not depend on the choice of O. However, computations in GAP shows that this is not the case. □

Proposition 4. *The group* `SmallGroup(625, 12)` *cannot act as an automorphism group of a Moore* $(57, 2)$*-graph* Γ *with the smallest orbit of size 25*.

Proof. Let us assume that $X =$ `SmallGroup(625, 12)` acts as an automorphism group of Γ with the smallest orbit of size 25.

First we sum up some fact about the group X, which has in GAP a polycyclic presentation in four generators f_1, f_2, f_3 and f_4. In this presentation, the centre of X is generated by f_3 and f_4 and the Frattini subgroup of X is generated by f_4. Every nonidentity element has order 5 and every non-central element has five conjugates. Consequently, any vertex stabilizer of an orbit of size 125 must fix 25 elements in this orbit and 50 elements in total.

There are 30 conjugacy classes of non-normal subgroups of order 25. One can choose representatives in such a way that each representative is generated by a pair u and v of elements where $u \in U = \left\{f_1, f_2, f_1f_2, f_1^2f_2, f_1^3f_2, f_1^4f_2\right\}$ and $v \in V \left\{f_3, f_3f_4, f_3f_4^2, f_3f_4^3, f_3f_4^4\right\}$. In all cases the core is generated by v. Therefore we have 10 orbits of size 25 and, for every $v \in V$, two orbits have core generated by v. By the pigeonhole principle at least one point of U lies in at least two representatives.

If some element $u \in U$ lies in two representatives, then it fixes 50 elements, five in each orbit of size 25 and 25 in each orbit of size 125 in which it fixes a point. Therefore u lies in five representatives and also fixes a point in exactly one orbit of size 125. The conjugates of u are $\left\{u, uf_4, uf_4^2, uf_4^3, uf_4^4\right\}$, therefore the elements $uf_3, uf_3^2, uf_3^3, uf_3^4$ have the same property as u, i.e., they fix a point in five orbits of size 25 and in one orbit of size 125. Thus X has at least five orbits of size 125.

Let O_1 be the orbit of size 125 in which u fixes some point and let O_j be a different orbit. If $|O_j| = 25$ and u fixes some point in O_j then $b_{1j} = 1$, otherwise $b_{1j} = 0$. If $|O_j| \geqslant 125$, then u fixes no point in O_j and $5|b_{1j}$. Moreover $\sum_j b_{1j}b_{j1} + b_{11} - 56 = 125$ and $\sum_j b_{1j} = 57$. Computations in GAP show, however, that such entries b_{1j} do not exist. □

Lemma 23. *Let X be an automorphism group of Γ of order* 625 *with the smallest orbit of size* 125. *Then X contains a subgroup Y of order* 5 *which is a vertex stabilizer in at least one and at most two orbits of size* 125.

Proof. Let O be an 125-element orbit of X and Y be the vertex stabilizer of a vertex $o \in O$. The pair $(|\mathrm{Fix}(Y)|, |\mathrm{Fix}(Y) \cap O|)$ is one of $(5,5), (50,5), (50,25)$. Depending on $(|\mathrm{Fix}(Y)|, |\mathrm{Fix}(Y) \cap O|)$, Y is a vertex stabilizer of exactly 1, 10, and 2 orbits, respectively. The statement now follows from the fact that the number of orbits of size 125 is congruent to 1 mod 5. □

Lemma 24. *Let X have order* 625 *and let the smallest orbit of X have size* 125. *Then X has at least two orbits of size* 125.

Proof. Let $x \in X$ be a central element of order 5. By Lemma 12, $a_1(x) > 0$. Therefore x contributes to at least one orbit O. Since x is central, Lemma 7 shows that $|O| \leq a_1(x)$, and $a_(x) \leq 500$ by Corollary 1. The orbit O therefore cannot have size greater than 500. Moreover, x and x^2 contribute to different orbits. □

Proposition 5. *The graph Γ does not admit a group of automorphisms of order* 625 *with the smallest orbit size* 125.

Proof. Let us assume that $|X| = 625$ and that X has a total of k orbits numbered in such a way that orbits $O_1, O_2, \ldots, O_i$ have size 625, $O_{i+1}, \ldots, O_k$ have size 125, and O_k is an orbit whose vertex stabilizer Y fixes elements from at most two orbits; its existence is guaranteed by Lemma 23).

Let $b_{k1}, b_{k2}, \ldots, b_{kk}$ be the kth row of the adjacency matrix B of X. Since each of the first i orbits has size 625 we have $125b_{kj} = 625b_{jk}$ for $1 \leqslant j \leqslant i$. If O_j is an orbit of size 125 such that Y does not fix a vertex in O_j and if $o \in O_k$ is fixed by Y, then Y acts semi-regularly on the neighbors of o in the orbit O_j, that is, b_{kj} is a multiple of 5. Hence, 5 divides all the entries $b_{k1}, b_{k2}, \ldots, b_{ki}$ and all but at most one entries among b_{kj} where $i + 1 \leq j \leq k - 1$. Considering the bottom right entry in the equation $B^2 + B - 56I = (1, 1, \ldots, 1)^T(s_1, s_2, \ldots, s_k)$ from Lemma 5 we obtain

$$\left(b_{k1}^2 + \ldots + b_{ki}^2\right)/5 + \left(b_{k,i+1}^2 + \cdots + b_{kk}^2\right) + b_{kk} = 181. \tag{9}$$

If $i \leqslant 3$, then computations shows that such b's do not exist. If $i = 4$, then there are six unordered possibilities for a row of the adjacency matrix for an orbit of size 125 (in all cases on the diagonal is 2).

$\{b_1, b_2, b_3, b_4\}$	$\{b_5, b_6, b_7, b_8, b_9, b_{10}\}$
{10, 10, 5, 5}	{5, 5, 5, 5, 5, 2}
{15, 10, 5, 5}	{5, 5, 5, 5, 2, 0}
{15, 15, 5, 5}	{5, 5, 5, 2, 0, 0}
{20, 10, 10, 5}	{5, 5, 2, 0, 0, 0}
{20, 15, 10, 5}	{5, 2, 0, 0, 0, 0}
{20, 15, 15, 5}	{2, 0, 0, 0, 0, 0}

According to the table we will say that orbit of type 125 is of type 1, 2, 3, 4, 5 or 6.

By Lemma 10, the trace of an orbit of size 625 is an even integer from $\{6, 8, 10, 12, 14\}$. The trace of X is congruent to 0 mod 60 and every orbit of size 125 has trace equal to 2. Therefore $\mathrm{Tr}(X) = 60$ and sum of traces of the orbits of size 625 equals 48.

If X contains an orbit of type 1 or 6, then it is impossible to find four rows of adjacency matrix corresponding to orbits of size 625. For type 2, no solution has sum of traces equal to 48. For types 3 and 5, every solution with sum of traces equal to 48 requires another orbit of type 6. Finally, for type 4, every solution with sum of traces equal to 48 requires at least one orbit of another type. □

9. Mixing the primes

Our goal – specification of possible automorphism groups of a Moore $(57, 2)$-graph of odd order – is facilitated by two classical results in group theory. By the Odd Order Theorem of Feit and Thompson, any group X under our consideration is solvable. Thus, by the result of Philip Hall (see [13]), whenever $|X| = ab$ for relatively prime a and b, X has a subgroup of order a. This enables us to approach the groups X 'from below' in the sense of the number of prime divisors.

The next step in our investigation is considering groups of automorphisms of Γ of non-prime-power order, in particular, of order $p^a q^b$ for distinct odd primes p, q and for $a, b \geq 1$. We recall that a Sylow p-subgroup of a group X of order $p^a u$ with $(p, u) = 1$ is any subgroup of X of order p^a. By Sylow's Theorem, the number of Sylow p-subgroups of X is congruent to 1 mod p and divides u.

In what follows let X be an automorphism group of Γ such that $|X| = p^a q^b$ where p, q are distinct odd primes and $a, b \geq 1$. Further, let P and Q be Sylow p- and q-subgroups of X, respectively.

Lemma 25. *If P is normal in X, then Q acts on orbits of P. In particular, Q acts as an automorphism group of* $\mathrm{Fix}(P)$.

Lemma 26. *In the above notation, $p \leqslant 5$ or $q \leqslant 5$.*

Proof. Suppose that $p, q \in \{7, 11, 13, 19\}$. Recall that, by Sylow's theorem, the number of distinct Sylow p-subgroups of a group of order $p^a q^b$ is a power of q congruent to 1 mod p; a similar remark applies to Sylow q-subgroups. Considering all possibilities listed in Lemma 19 it follows that both P and Q must be normal in X, that is, X is the direct product of P and Q. Therefore P acts on the set of fixed points of Q and vice versa. This is clearly possible only if $p = 7$, $q = 19$, $P \cong \mathbb{Z}_7$, and $|\mathrm{Fix}(P)| = 58$, which contradicts Lemma 12. □

Proposition 6. *Let $p = 3$ and $q = 5$. Then $Q \trianglelefteq X$. Moreover,*

(1) *if $P \trianglelefteq X$, then $|\mathrm{Fix}(P)| = 10$, $|\mathrm{Fix}(Q)| = 0$, and $|Q| = 5$;*
(2) *if $P \not\trianglelefteq X$, then $|P| = 3$ and $Q \in \{\mathbb{Z}_5^2, \mathbb{Z}_5^3, \mathbb{Z}_5^2 \cdot \mathbb{Z}_5\}$.*

Proof. Since $|P|$ divides 27, normality of Q follows from Sylow's Theorem.

Now, assume that $P \trianglelefteq X$, that is, $X = P \times Q$, and consider a cyclic subgroup $Y \leq X$ of order 15. Let P' and Q' be the Sylow subgroups of Y. Then, $\mathrm{Fix}(P')$ is the Petersen graph and is a union of orbits of Q'. Similarly, $\mathrm{Fix}(Q')$ is a union of orbits of P'. As an automorphism of order 5 of the Petersen graph acts semi-regularly on vertices, we have just two possibilities: either $\mathrm{Fix}(Q')$ is empty, or $\mathrm{Fix}(Q')$ is the Hoffman-Singleton graph and $\mathrm{Fix}(P') \subset \mathrm{Fix}(Q')$. The second possibility, however, cannot occur because an automorphism of order 3 in the Hoffman-Singleton graph cannot have exactly 10 fixed points.

If $P \not\trianglelefteq X$, then P acts on Q and the preceding arguments show that this action is faithful. From the 5-groups of order at most 125 only $\mathbb{Z}_5^2$, $\mathbb{Z}_5^3$, and $\mathbb{Z}_5^2 \cdot \mathbb{Z}_5$ have an automorphism of order 3. In addition, in all three cases the Sylow 3-subgroup of the automorphism group has order 3. □

Proposition 7. *Let $p = 3$ and $q > 5$. Then $q \neq 11$, $Q \trianglelefteq X$, and $P \not\trianglelefteq X$. If $q = 19$, then $|P|$ divides 9, and if $q \in \{7, 13\}$, then $|P| = 3$.*

Proof. If $q \neq 13$, normality of Q in X follows from Sylow's Theorem as in the previous proof. As P contains an element of order 3 fixing a copy of the Petersen graph with automorphism group of order 120, P cannot be normal in X.

If $q = 13$, then P cannot be normal in X because $\mathrm{Fix}(P)$ does not have an automorphism of order 13. If $Q \not\trianglelefteq X$, then X can only be the extension of $\mathbb{Z}_3^3$ by the automorphism of order 13. In this case, however, $P \trianglelefteq X$ – a contradiction.

Consequently, for any q the group P acts faithfully as a group of automorphisms on Q. If $Q = \mathbb{Z}_7^2$, then every element of P can be identified with a 2×2 matrix over $\mathbb{Z}_7$. If $|P| = 9$, then P contains a matrix $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 2 \end{smallmatrix}\right)$ which fixes the element $(1, 0) \in Q$. In other words, X contains a cyclic subgroup of order 21, which is not possible. □

Proposition 8. *Let $p = 5$ and $q > 5$. Then $q \in \{7, 11\}$ and $Q \trianglelefteq X$. If $q = 11$, then $|P|$ divides 25. If $q = 7$, then $P \trianglelefteq X$ and $|X| = 35$.*

Proof. Again, Sylow's Theorem provides normality of Q in X and also normality of P in X if $q \neq 11$. Therefore, if $q \neq 11$ then $X = P \times Q$.

Let $q = 19$. As Q fixes exactly one point, $\mathrm{Fix}(P)$ is non-empty and has an automorphism of order 19 – a contradiction.

Let $q = 13$. Since $X = P \times Q$, it contains an element x of order 65. Such an automorphism, however, cannot exist by Lemma 15.

Let $q = 7$. By Lemma 19, $\mathrm{Fix}(Q)$ is a star and hence $\mathrm{Fix}(P)$ is non-empty. Since a pentagon does not have an automorphism of order 7, $\mathrm{Fix}(P)$ must be the Hoffman-Singleton graph and $|P| = 5$. As a group of order 49 cannot fix a single vertex in the Hoffman-Singleton graph, we conclude that $|Q| = 7$ and, by Lemma 15, $|\mathrm{Fix}(Q)| = 16$.

Finally let $q = 11$. As Q is normal in X, P act as a group of automorphisms of Q. Let P' be the kernel of this action. It suffices to show that $|P'|$ divides 5.

First, we show that for any element $y \in P'$ we have $\mathrm{Fix}(y) = \mathrm{Fix}(Q)$. As y centralizes Q we have $\mathrm{Fix}(y) \subseteq \mathrm{Fix}(Q)$. If $\mathrm{Fix}(y) = \emptyset$, then the group $\langle y \rangle \times Q$ has on Γ one orbit of size 5 equal to $\mathrm{Fix}(Q)$ and 59 orbits of size 55. As $\mathrm{Fix}(Q)$ is a pentagon, exactly one of y and y^2 contributes to the orbit $\mathrm{Fix}(Q)$. As other orbits have size 55 we obtain $a_1(y) \neq a_1(y^2)$ which is a contradiction with Lemma 11.

Let $|P'| > 1$. By Lemma 13, P' does not contain an element of order 25. As every nonidentity element of P' has order 5 we have $\mathrm{Fix}(P') = \mathrm{Fix}(Q)$ and P' acts semi-regularly on $\Gamma \setminus \mathrm{Fix}(Q)$. Therefore $|P'| = 5$. □

Remark. The preceding results show that if x is an automorphism of Γ of odd order pq, then x is covered by Lemma 15. Automorphisms of order $2p$, p odd, can be handled by similar arguments in combination with the results of Makhnev and Paduchikh.

Now we are ready to prove our main results.

Theorem 6. *Let Γ be a Moore graph of degree 57 on 3250 vertices and $G = \mathrm{Aut}(\Gamma)$. If $|G|$ is odd then $|G|$ divides $19 \cdot 3^2, 13 \cdot 3, 5^2 \cdot 11, 7^2 \cdot 3, 7 \cdot 5, 5^3 \cdot 3$, or $3^3 \cdot 5$.*

Proof. If G has at most two prime divisors, then its size lies in the list above. By the facts mentioned earlier it suffices to show non-existence of G with $|G|$ having three prime divisors. By Propositions 6, 7 and 8 the only possibility for the odd part of G is the direct product of $\mathbb{Z}_5$ and $\mathbb{Z}_7 \cdot \mathbb{Z}_3$. However, by Lemma 15 the element of order 5 in such a group G fixes simultaneously the Hoffman-Singleton graph and the empty set. □

Finally, applying our methods to possible groups of automorphisms Γ of even order we are able to improve the earlier results of Makhnev and Paduchikh.

Theorem 7. *Let Γ be a Moore graph of degree 57 on 3250 vertices and $G = \mathrm{Aut}(\Gamma)$. If $|G|$ is even then $|G|$ divides $11 \cdot 5 \cdot 2, 5^2 \cdot 2, 3^3 \cdot 2$, or $2p$, $p \in \{7, 11, 19\}$.*

Proof. By Theorem 2 $G = Y\langle t \rangle \times X$ where t is an involution and X and Y have odd order. In their proof, Makhnev and Paduchikh showed that any automorphism of order 3 in Y fixes exactly one point which is not possible. By Theorem 5 if $\mathrm{Fix}(X)$ is the Hoffman-Singleton graph, then $|X| \neq 25$. Finally, by Lemma 15 G cannot contain $\mathbb{Z}_{55}$ an d $\mathbb{Z}_{22}$ with common subgroup of order 11 or $\mathbb{Z}_{10}$ and $\mathbb{Z}_{35}$ with common subgroup of order 5. □

Corollary 3. *Let Γ be a Moore graph of degree 57 on 3250 vertices and $G = \mathrm{Aut}(\Gamma)$. Then, $|G| \leqslant 375$, and if $|G|$ is even, then $|G| \leqslant 110$.*

10. Conclusion

By the time of writing this article, progress in the research into symmetries of the Moore $(57, 2)$-graph(s) was achieved mostly by studying properties of individual automorphisms. Higman (see [3]) successfully used methods of linear algebra, whereas tools developed by Makhnev and Paduchikh [10] are of combinatorial and group-theoretical nature. In our investigation we have combined all the previous methods, enriched by equitable partitions and supported by the use of computers. We feel that our main contribution lies in studying entire subgroups rather than single automorphisms, focusing on ways the automorphisms within a subgroup influence each other.

Thanks to Makhnev and Paduchikh [10] it was sufficient to restrict ourselves to groups of odd order, the Odd Order Theorem with results of Philip Hall thus enabled us to study possible automorphism groups of the Moore $(57, 2)$-graph(s) in terms of the number of prime divisors of their orders. Our upper bounds on possible orders of p-groups led to the finding that in groups of order $p^a q^b$ at least one of the Sylow subgroups is normal. This was the main step towards completion of characterization of possible orders of automorphism groups of the graph(s). As a matter of fact, with the exception of 110, all possible orders have at most two distinct prime factors.

The choice of the form of presentation of our main results was determined by trying to avoid unnecessary technical details and preferring compactness of statements. In particular, restrictions on orders of groups acting on the Moore $(57, 2)$-graph(s) are not the strongest pieces of information we are able to derive. Our methods enable one to substantially restrict the values of the functions a_0 and a_1, and hence the orbit structure of the actions. For example, from Lemma 15 it follows that there is no automorphism of order 110.

On the one hand, it is possible that some of the orders listed in our two main theorems could be excluded by showing non-existence of suitable adjacency matrices for groups of automorphism, as done for the order 625 in section 8. On the other hand, in the study of possible actions of groups of order 375 with 10 orbits we found hundreds of matrices satisfying conditions of Lemma 5 which we were not able to exclude by our techniques. An example of such a matrix is:

$$\begin{pmatrix} 2 & 5 & 8 & 10 & 6 & 8 & 5 & 6 & 4 & 3 \\ 5 & 8 & 8 & 3 & 8 & 6 & 8 & 7 & 4 & 0 \\ 8 & 8 & 6 & 6 & 2 & 4 & 9 & 7 & 3 & 4 \\ 10 & 3 & 6 & 6 & 8 & 5 & 4 & 10 & 3 & 2 \\ 6 & 8 & 2 & 8 & 10 & 5 & 8 & 5 & 2 & 3 \\ 8 & 6 & 4 & 5 & 5 & 12 & 7 & 6 & 2 & 2 \\ 5 & 8 & 9 & 4 & 8 & 7 & 4 & 8 & 0 & 4 \\ 6 & 7 & 7 & 10 & 5 & 6 & 8 & 8 & 0 & 0 \\ 12 & 12 & 9 & 9 & 6 & 6 & 0 & 0 & 2 & 1 \\ 9 & 0 & 12 & 6 & 9 & 6 & 12 & 0 & 1 & 2 \end{pmatrix}.$$

We therefore think that one of the challenges for future research is to develop methods to deal with such situations.

For those believing in the existence of the Moore $(57, 2)$-graph(s) Γ, our methods point at promising places to look for candidates. Regarding symmetries, the theoretically best possible negative result would be to show that the automorphism group of Γ is trivial. In the course of our investigation we discovered a number of configurations that can appear in Γ. A study of such configurations could be of interest for researchers, even for those believing in the non-existence of Γ. Examples of such configurations are 15 mutually non-adjacent copies of the Hoffman-Singleton graph, and 11 copies of the Hoffman-Singleton graph sharing a pentagon.

Acknowledgments

Research of the first author was supported by the APVV Research Grant No. 0111-07 and the VEGA Research Grants No. 1/0588/09 and 1/0406/09. Research of the second author was supported from the APVV Research Grants No. 040-06 and 0104-07, the LPP Research Grants No. 0145-06 and 0203-06, and the VEGA Research Grant No. 1/0489/08. The first author would like to thank the Open University for hospitality during his research visit that initiated the work on this paper.

References

[1] M. Aschbacher, The nonexistence of rank three permutation groups of degree 3250 and subdegree 57, J. Algebra 19 (3) (1971) 538–540.
[2] E. Bannai, T. Ito, On finite Moore graphs, J. Fac. Sci., Univ. Tokyo, Sect. I A 20 (1973) 191–208.
[3] P. Cameron, Permutation Groups, Cambridge University Press, 1999.
[4] C.W. Curtis, I. Reiner, Representation Theory of Finite Groups and Associative Algebras, Wiley, 1988.
[5] R.M. Damerell, On Moore graphs, Math. Proc. Cambridge Philos. Soc. 74 (1973) 227–236.
[6] J.D. Dixon, B. Mortimer, Permutation Groups, GTM 163, Springer, 1996.
[7] The GAP Group, GAP — Groups, Algorithms, and Programming, Version 4.4.10, 2007, <http://www.gap-system.org>.
[8] C.D. Godsil, Algebraic Combinatorics, Chapman and Hall, 1993.
[9] A.J. Hoffman, R.R. Singleton, On Moore graphs with diameters 2 and 3, IBM J. Res. Dev. 4 (1960) 497–504.
[10] A.A. Makhnev, D.V. Paduchikh, Automorphisms of Aschbacher graphs, Algebra Logic 40 (2) (2001) 69–74.
[11] M. Miller, J. Širáň, Moore graphs and beyond: a survey of the degree/diameter problem, Electron. J. Combin., Dynamic Survey DS14 (2005), 61 pp.
[12] B. Mohar, Graph Laplacians, in: Beineke, Wilson (Eds.), Topics in Algebraic Graph Theory, Cambridge University Press, 2004, pp. 113–136.
[13] J.J. Rotman, An Introduction to the Theory of Groups, GTM 148, fourth ed., Springer, 1999.